

Testimony of James A. Baker, Counsel for Intelligence Policy
Office of Intelligence Policy and Review
United States Department of Justice
Committee on the Judiciary, before the
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives
April 26, 2005

Chairman Coble, Ranking Member Scott, and Members of the Subcommittee:

I am pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, I appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA under the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from happening again.

As Counsel for Intelligence Policy in the Department of Justice, I am head of the Office of Intelligence Policy and Review (OIPR). OIPR conducts oversight of the intelligence and counterintelligence activities of the Executive Branch agencies including the FBI. We prepare all applications for electronic surveillance and physical search under FISA and represent the government before the Foreign Intelligence Surveillance Court (FISA Court). OIPR reports directly to the Deputy Attorney General. I am a career member of the Senior Executive Service, not a political appointee.

I. FISA Statistics

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the FISA Court has dramatically increased.

- In 2000, 1,012 applications for surveillance or search were filed under FISA. By comparison, in 2004 we filed 1,758 applications, a 74% increase in four years.
- Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the Court in some substantive way.

II. Key Uses of FISA Authorities in the War on Terrorism

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical search authorized regarding suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information

on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the Department asks you to reauthorize the USA PATRIOT Act provisions scheduled to expire at the end of this year. Today, it is my understanding that the Committee wishes to discuss sections 204 and 207 of the USA PATRIOT Act. These provisions are scheduled to sunset at the end of the year. In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a “lone wolf” provision that expands the definition of “agent of a foreign power” to include a non-United States person who engages in international terrorism or in activities in preparation therefor and is not known to be affiliated with a larger group. This provision is also scheduled to sunset at the end of this year, and the Department asks that it be reauthorized as well.

A. Section 204 “Clarification of Intelligence Exceptions from Limitations on Interceptions and Disclosure of Wire, Oral and Electronic Communications”

Section 204 of the USA PATRIOT Act amended Title 18, United States Code, Sec. 2511(2)(f) in two ways. First, it provides that chapter 206 of title 18, which governs the installation and use of pen registers and trap-and-trace devices, is not intended to interfere with certain foreign intelligence activities that fall outside of the definition of “electronic surveillance” in FISA. Second, section 204 provides that the exclusivity provision in section 2511(2)(f) of title 18 applies not only to the interception of wire and oral communications, but also to the interception of electronic communications. Section 2511(2)(f) reflects Congress’s intent, when it enacted FISA and the Electronic Communications Privacy Act of 1986, to make the procedures in chapter 119 of title 18 (“Title III”) (regulating the interception and disclosure of wire, electronic, and oral communications), chapter 121 of title 18 (regulating access to stored wire and electronic communications and transactional records), and FISA (regulating electronic surveillance undertaken to acquire foreign intelligence information) the exclusive procedures for conducting electronic surveillance, as defined by FISA, and intercepting certain types of domestic communications.

Section 204 remedies an apparent omission in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, which, among other things, amended chapter 119 of title 18 (“Title III”) to provide procedures for intercepting electronic communications and added chapter 121 to title 18 to provide procedures for accessing stored electronic communications, but neglected to make a corresponding change to clarify that the exclusivity provisions in section 2511(2)(f) applies to the interception of not only wire and oral, but also electronic, communications.

Section 204 has been criticized by some opponents of the USA PATRIOT Act. For instance, some have argued that the section amended Title III and the Stored Communications Access Act so that stored voice-mail communications, like e-mail, may be obtained by the government through a search warrant rather than through more stringent wiretap orders. These critics, however, confuse section 204 with section 209 of the Act.

In reality, section 204, as the nonpartisan Congressional Research Service has observed, is “essentially a technical amendment” that merely clarifies what Congress had always intended

the statute to mean. In an age when terrorists use electronic communications just like everyone else, it is important to preserve section 204.

B. Authorized Periods for FISA Collection

Section 207 of the USA PATRIOT Act has been essential to protecting the national security of the United States and protecting the civil liberties of Americans. It changed the time periods for which some electronic surveillance and physical searches are authorized under FISA, and in doing so, conserved limited OIPR and FBI resources. Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources can be devoted to other investigative activity as well as conducting appropriate oversight of the use of intelligence collection authorities at the FBI and other intelligence agencies. A few examples of how section 207 has helped are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct physical search regarding any agent of a foreign power for periods of up to 90 days. Section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods for electronic surveillance and physical search equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the Senate Judiciary Committee earlier this month, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of applications. Because of section 207's success, the Department has proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow coverage of a non-U.S. person for 120 days initially with each renewal of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission. The WMD Commission

agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

C. The “Lone Wolf” Provision

In addition to the USA PATRIOT Act provisions scheduled to sunset at the end of this year, the “lone wolf” provision of the Intelligence Reform and Terrorism Prevention Act of 2004 is also scheduled to sunset. Before passage of this provision, FISA prevented the FBI from obtaining a surveillance order of an international terrorist unless it could establish a connection to a foreign power. However, a lone wolf terrorist seeking to attack the United States may not be connected to a foreign power, or his connection to a foreign power may not be known. This provision applies only to non-U.S. persons engaging or preparing to engage in international terrorism, and FISA Court authorization is still required to monitor lone wolf terrorists.

Senator Schumer stated during the Senate debate on the lone wolf provision: “Right now we know there may be terrorists plotting on American soil. We may have all kinds of reasons to believe they are preparing to commit acts of terrorism. But we cannot do the surveillance we need if we cannot tie them to a foreign power or an international terrorist group. . . . It makes no sense. The simple fact is, it should not matter whether we can tie someone to a foreign power. . . . Engaging in international terrorism should be enough for our intelligence experts to start surveillance.”

A lone wolf, or one who appears to be a lone wolf, may have the capacity to cause grievous harm to America and her citizens, and the threat posed by lone wolf terrorists will not disappear at the end of this year. Therefore, the Department requests that this provision be made permanent.

CONCLUSION

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. The USA PATRIOT has greatly enhanced the ability of OIPR, as well as prosecutors, the FBI, and the Intelligence Community, to effectively wage the war on terrorism.

I thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation’s ongoing war against terrorism. I appreciate the Committee’s close attention to this important issue. I would be pleased to answer any questions you may have. Thank you.